Addressing The Concern of Malicious Drone in The Internet of Drone Sixth Generation Mobile System Powered by WSNs Using Three Security Levels

Ahssan Ahmed Mohammed Lehmoud[1],
Fadhil Mohammed Salman[1,*], Mohamed Q. Mohamed[1],
Fanar Ali Joda[2] and Mohammed Hasan Aldulaimi[3]

[1]*Ministry of Education, Babylon Education Directorate, Iraq*
[2]*Department of Air Conditioning & Refrigeration Engineering Techniques, Al-Mustaqbal University, Iraq. Ministry of Education, Babylon Education Directorate, Babylon, Iraq*
[3]*Department of Computer Techniques Engineering, Al-Mustaqbal University, Iraq*
E-mail: ahssan_ahsan@bab.epedu.gov.iq; fadhilmohammad2023@bab.epedu.gov.iq; moh.swd1988@gmail.com; fanaralijoda@uomus.edu.iq; mohammed.hassan@uomus.edu.iq
[*]*Corresponding Author*

Received 21 June 2024; Accepted 20 September 2024

Abstract

Securing communications in drone networks is an essential aspect of ensuring good network performance. Data transferred over the Internet of Drones (IoD) Communications, which is rapidly growing, holds crucial information for navigation, coordination, data sharing, and control, and enables the creation of smart services in many sectors. Sixth-generation (6G) mobile systems are anticipated to be impacted by the plethora of IoD. The possibility of malevolent drones intercepting or altering data before it reaches its target is a serious worry. Operations on IoD networks may be hampered

Journal of Cyber Security and Mobility, Vol. 13_6, 1449–1466.
doi: 10.13052/jcsm2245-1439.13610

by this, and safety issues may arise. Utilizing three security levels, the suggested method solves the issue of malicious drones in the IoD network. The suggested system's first level allocates a trust value to IoD drones based on behaviors including prior drone behavioral histories, packet losses, and processing delays. This can be accomplished by choosing drones as investigators to monitor the actions of neighboring drones and assess the level of trust value. The second level involves communication protection, which is accomplished by historical communication behavior. The purpose of the final security level is to safeguard the reliability of the data used to calculate trust values. The fundamental topical of our proposed system is to propose and explore a novel tactic for detecting malicious UAVs within the internet of drone framework, using theoretical and simulations models. Because that 6G networks are still now in the developmental stage, the results presented are based on predictive analyses and simulations rather than real-world applications.

Keywords: Security, malicious drones, IoD, 6G network, trust value, PDR.

1 Introduction

Recently, most of the smart devices have been connected to the internet such as wireless sensors, smartphones, smart home lights and accessories, cars, etc. The Internet of Things has developed services in many areas such as smart homes and cities, retail, smart transportation, etc [1]. Certainly, in the near future, the Internet of Things will be highly dependent on sixth-generation (6G) networks. Where the sixth generation network will form the infrastructure for connecting a huge number of applications and smart devices, with a very high data transfer rate [2]. 6G will certainly overcome all the weaknesses of the networks of previous generations. Furthermore, 6G is anticipated to satisfy the needs of the future completely wired digital society [3]. The 6G-enabled IoT systems, which involve self-driving, squadrons of drones, virtual reality devices, bio-sensors and telepresence, will undergo a significant technological transformation [4, 5], and [6].

Botnets are considered the most dangerous, most difficult, and most influential cyber menace among all IoD assaults; in comparison to other attacks, it can have a significant impact [7]. Millions of Internet of Things (IoT) devices were the target of a new botnet named BotenaGo, which was exposed by ATT security researchers in 2021 [8, 9], and [10]. Botnets are frequently developed for a variety of harmful activities, including distributed denial-of-service

(DDoS) attacks, information and identity theft, huge spamming and phishing [11, 12].

IoD enables serviced-based huge commutation topologies to be supported on 6G networks [13]. Our recommendation can also be quite helpful in controlling dynamic flow and minimizing attacks. Additionally, it offers a multi-level trust-based security system at 6G IoD to guarantee a seamless and secure data transfer between linked drones.

Though various studies have concentrated on the coupling some key networks and ML/DL, several network enablers are important for securing IoT networks [14], this survey expands on earlier efforts by offering developing solutions, including major enablers. However, large-scale cyber attack detection, avoidance and mitigation measures for IoD security have not been widely conducted in any previous surveys. Furthermore, the probability of 6G network to secure large IoD and develop the next-generation IDS with dynamic scenario adaptation in enormous IoD networks has not been examined in previous surveys.

This paper is organized as follows: A full account of the study's related literature will be provided in Section 2. Full details of the proposed framework (system components, requirements, and validation evaluation processes) are provided in Section 3. The system's performance evaluation and the experimental findings are illustrated in Section 4. Sections 5 and 6 wrap up the essay and propose possible directions for further research.

2 Literature Survey

Several excellent surveys articles, tutorials, and reviews focusing on drone connection networks using B5G/5G have been proposed during the previous six years [15, 16]. Table 1 presents an overview of the most recent and well-read articles in this field.

Li et al. [15] performed a thorough analysis of drone telecommunication over B5G/5G wireless network. From the perspectives of the network layer, physical layer, caching, computing, and cooperative communication, the authors provided a summary of modern researches activities on drone telecommunications integrating B5G/5G techniques. The researchers also considered the same open research challenges in an effort to create a strong foundation for drone implementation in 5G/B5G networks.

In a tutorial study published by Zeng et al. [17], some difficulties in drone communication over wireless networks exceeding 5G were covered. The issues that were emphasized were particular channel characteristics and

Table 1 1 Gen to 6 Gen – important execution metrics

Net-Gen	Techniques	Basic-Net	Freq-Range	Rate of Data	Navigation Range	Power Efficient	Latency
1G	– AMPS – MTS – PPT – IMTS	PSTN	825–895 MHz	2.4 Kbps	–	–	More than 1000 milliseconds
2G	– IS-95 – GSM – CDMA – EDGE	PSTN	850–1900 MHz	64 Kbps	100 km/h	0.01 J	500 milliseconds
3G	– IMT2000 – WCDMA – UMTS – CDMA2000 – TD-SCDMA	Packets N/W	1.8–2.5 MHz	2 Mbps	150 km/h	0.1 J	100 milliseconds
4G	– LTE – WiMAX – LTE-A	Internet	2.8 MHz	1 Gbps	350 km/h	1 J	50 milliseconds
5G	– 5G-NR – IPv6 – OFDM	IoT	– Sub-6 MHz – Mm Wave for fixed access	10 Gbps	500 km/h	10 J	5 milliseconds
6G	– GPS – COMPASS – GLONASS – Galileo	IoE	– Explore of THz band (over 500 GHz) – Sub-6 MHz – RF (eg. VLC, Optical, etc.)	1 Tbps	1000 km/h	>100 J	Less than 1 milliseconds

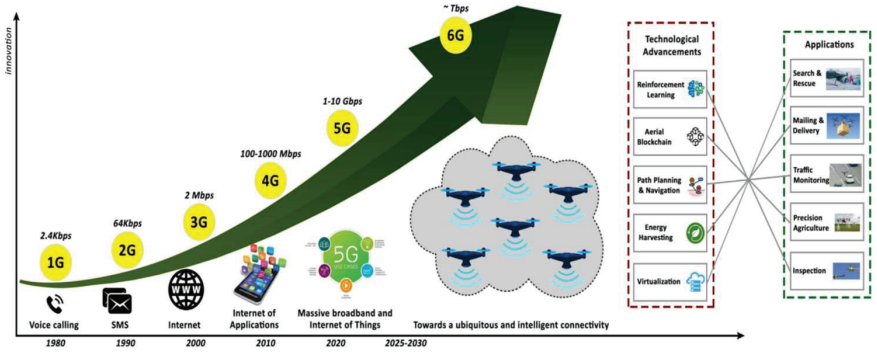

Figure 1 Compares cellular communication with modern technology for a variety of drone uses.

special requirements for communication. Additionally, significant drone network difficulties such, high altitude, quick 3D mobility, and battery depletion have been researched.

Fotouhi et al. [18] defined a review that addressed the bulk of the elements that facilitate the effortless incorporation of drones in cellular-net. Newer network, including 5G, is anticipated to be better prepared to handle drone-related challenges.

Recent developments in drone networking and communication technology were covered by Sharma et al. [19]. The usage of centralized and decentralized approaches to both algorithm-based software and hardware, as well as drone communication systems, are all examined in this work. It was expected that the advent of 5G technology will result in networks that are more reliable and stable.

The most recent developments in the integration of drone networks into B5G and 5G technologies have been studied by Ullah et al. [20]. The research team also looked into drone standardization, collision prevention, channel modeling and interference avoidance. Privacy and security conditions, in addition to deep reinforcement learning methods for investing in ideal trajectory planning and power harvest methods in UAV-net usage B5G and 5G approaches, are completely examined.

The difficulties and significance of incorporating drones into B5G/5G networks were examined by Sanchez et al. [21].

Blockchain-assisted secure drone interaction across 6G mobile networks was proven by Gupta and et al. [22]. The same work also discusses architecture, study challenges, and potential future ways for advancement.

Khan and et al. [23] examined mobile edge computing (MEC) and 5G networks for communication as potential solutions for enabling drone-enabled ecosystems and resolving core drone network issues such as limited processing, coverage, and storage. They discussed the newest developments and made an effort to address some of the most pressing issues as they discussed the 5G and MEC alternatives. In addition, they brought out fresh security concerns in light of the recent rise in popularity of drone communication networks. The work also examined developments in the drone sector that enable the application of all the mentioned advances.

Wu and et al. [24] They broadly reviewed recent scientific areas on drones integration in the cellular-net, with an interest in utilizing modern approaches like intelligent brief packet transfer, power harvesting, reflective surface, radars sensing, joint interaction and edge smart to achieve the variety services supplies of the following wireless techniques generation. Additionally, the researchers indicated crucial lines of inquiry for future research.

A WI-enabled drone using a new 6G radio operating in the not licensed spectrum, suggested by Orikumhi and et al. [25] might be utilized as a sink, relay or point of data gathering and dissemination. The researchers of this work have categorized drones according to their traits, operations, purposes, and functions. Drone integration with the cellular network is being researched through a number of regulatory and standardization initiatives. They discuss a number of NR-drone prospects, design challenges for WI drones, and potential future applications for WI drones.

Recent research by Amodu and et al. [26] examined the prospects and applications cases for THz-powered drone techniques using 6G-nets, in addition to the special design restrictions and tradeoffs associated to them. Researchers covered current advancements in THz standardize, drone activation regulations, and THz united health issues.

3 The Proposed Authentication Model

In an IoD, trust administration models have been suggested as a workable defense versus malignant drones. Where, trust administration models can be created for many different purposes. The suggested trust administration model was created to recognize malignant drones that either drop data rather than delivering it to the target or delay data before delivering it to the final location. These were determined to be the best criteria for identifying assaults because various malicious attacks result in drones packets being dropped or delayed within the IoD. But as the two measurements depend on the state of

the network, decisions had to be made. The suggested approach would take into account a further drone history metric, which will describe the behavior of the drones during earlier communication cycles. Even though the drones are not malicious, unstable network circumstances might nevertheless cause data to be dropped or delayed. Due to this, harmless drones are mistakenly identified as dangerous ones by the IoD.

3.1 Components of the Authentication System

The elements listed below will make up the suggested authentication strategy.

1. Drones: represents the group of the drones are held by the IoD. They have the ability to interact both with the infrastructure and with other drones in the IoD.
2. Authentication data: IoD drone data is created using lightweight data. Only drones with the watchdog active agent can create them.
3. IoD agent: This agent can be utilized to uav to enable monitoring procedure. The watchdog agent is responsible for monitoring uav data to sending to the RSU. The watchdog have ability to data collected from readily available network information. In case an uavs has recently joined the internet of drone and information is not available, then the watchdog agent will forward trust of data in order of create data on uav. Only verified trusted uavs are selected as watchdogs in the internet of drones and only watchdogs are permitted to monitor data on uavs. This significantly reduces the risk of uavs bad-mouthing with other uav in the IoD.
4. IoD: The IoD can be in one of the three modes. In the initial mode, there are no malicious drones operating in the IoD. This is used to establish a baseline for the IoD under ideal operating conditions. In the second mode, The IoD will be full of malicious drones, and this case includes the attitude of the IoD in the existence of malignant drones. The third mode includes applying the suggested approach with the presence of a number of malicious drones. The objective of this mode is to verify the performance of the suggested approach in a IoD that has malicious drones.

Architecture for authentication In this scenario, an area (A) has been covered by a drone network. Whenever a group of drones (Dn) are spread out at random:

$$(\mathrm{D_n}) \text{ here, } \mathrm{n} = \{1, 2, 3, \ldots, \mathrm{X}\} \text{ and } \mathrm{n} \in \mathrm{X} \tag{1}$$

Drones interact with each other as well as interact with a number of network modules (NM):

$$(\mathrm{NM}) \text{ here, } \mathrm{M} = \{1, 2, 3, \ldots, \mathrm{Y}\} \text{ and } \mathrm{M} \in \mathrm{Y} \tag{2}$$

Within the IoD, a collection of at least two watchdogs ($\mathrm{D0_{NO}}$) exists like the following:

$$(\mathrm{D0_{NO}}) \text{ here, } \mathrm{NO} = \{1, 2, \ldots, \mathrm{X}\} \text{ and } \mathrm{D0_{NO}} \in \mathrm{D_{NO}} \text{ and } \mathrm{NO} \in \mathrm{X} \tag{3}$$

The suggested method has taken into account data integrity, consistency factor packet delivery ratio (PDR), and history when evaluating authentication. Before delivering the chosen metrics to the central IoD agent to determine the authentication value, the network of drone IoD agents monitors them from the drones. The equations and procedures listed below are used to calculate the authentication metrics.

$$\mathrm{PDR(D_n)} = \sum_{NO}^{n} \frac{Ax}{TY} \tag{4}$$

Here : X = {1, 2, 3,. . . , X}, Y = {1, 2, 3,. . . ,Y}, I = {1, 2, 3,. . . , I} & X,Y, I ∈ N

$$\mathrm{DP(D_n)} = \sum_{NO}^{n} \frac{\lambda_x - \gamma_y}{x} \tag{5}$$

Here: DP is delay processing, X = {1, 2, 3,. . . , X}, Y = {1, 2, 3,. . . , Y}, n = {1, 2, 3,. . . , NO} & X, Y, n ∈ NO

Algorithm 1: Performing an authentication value matrix (AVm) estimation

Inputs: drone map: ($\mathrm{D_n}$, $\mathrm{N_s}$), θ, β
Outputs: (AVm) to each ($\mathrm{D_n}$)
While time ∈ T do
AVM:
Elect D'n from $\mathrm{D_n}$
If $\sum_{NO}^{n} D_n$ (Ty ≥ Az) then
Compute PDR($\mathrm{D_n}$) based on Model (4)
End if
If $\sum_{NO}^{n} D_n$ (λx ≥ γy) then
Compute PD($\mathrm{D_n}$) based on Model (5)

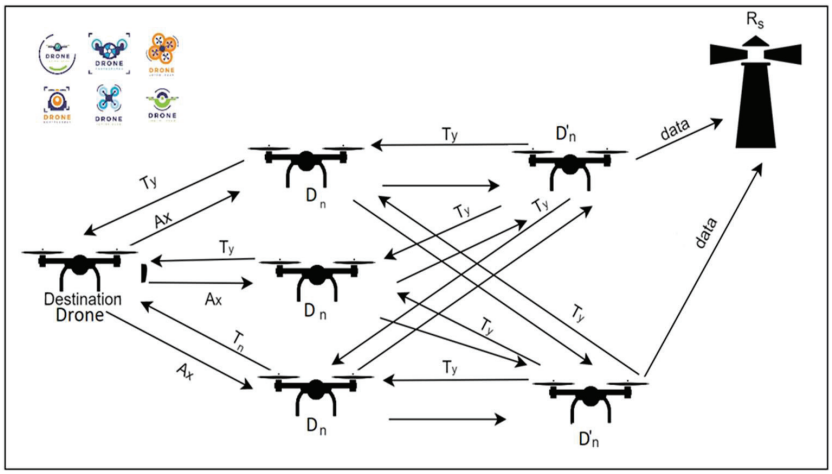

Figure 2 Shows a simulation scenario illustrating how the suggested approach work.

End if
For D'n $\in$ D_n do
Update authentication matrix AVm(D_n) based on Model (3)
End for
End while

Figure 2 depicts the IoD topology and interactions. If information about the drones (D'n) is easily accessible, the IoD agent (D'n) will gather it and deliver it to the roadside unit (Rs). In the event that data is unavailable, (D'n) should transmit authentication (Ay) to the drones (Dn). The data will be forwarded via (Dn) to the target drone, which will reply with an acknowledgement (Ax) after receiving it (Ay). As (D'n) observe these interactions, (Rs) receives drone information.

4 Simulation and Experiments Results

The OMNET++ simulator was used to assess the effectiveness of the suggested authentication approach. The suggested approach is tested to demonstrate its usefulness. The suggested approach is subjected to a variety of scenarios, including those involving malicious drones that are delaying packet, dropping packet and scenario where malignant drones are doing both. The threat agent will simulate malicious behavior in a sample of randomly chosen IoD network drones. This will be used to gauge how well

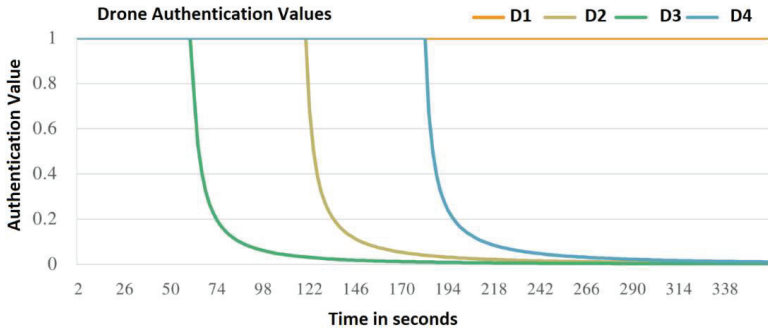

Figure 3 Drone authentication values with existing malicious drones dropping data into the IoD.

the suggested approach will detect drones acting maliciously. In the IoD network, three distinct kinds of malicious drones will be simulated. The suggested approach is initially tested on an IoD made up of drones that behave maliciously and non-maliciously. The drone will drop data in the IoD at varying rates as part of malicious action.

Figure 3 displays the outcomes of the evaluations of the (D1, D2, D3, and D4) drones. Due to the fact that D1's authentication value remained constant at 1.0 during the IoD process, it was determined that it was not acting maliciously. Due to the fact that the authentication values of (D3, D2, and D4) decreased during the IoD process, so these drones (D3, D2, and D4) are believed to behave maliciously. The drones are recognized as dropping packets while participating in IoD operations. This demonstrates that the suggested approach is effective at differentiating between malicious and non-malicious drones when the latter display their actions of dropping packets.

The suggested approach will be tested in the second experiment against malicious drones that are intentionally delaying data in the IoD. Different drones will delay data in the IoD at various times.

In the third experiment, multiple types of malicious drones were applied to the IoD. The malicious behaviors would include either dropping packets, delaying packets, or both dropping and delaying packets.

The suggested approach will be examined in the fourth experiment for potential 6G mistakes and false-positives in the IoD. This assesses how well the suggested approach is able to distinguish between malicious and non-malicious behavior. Data delivery from drones may take longer or may be lost (dropped) due to 6G issues. False positives results may result from this. False

positives occur when a drone is recognized as being malicious but behaves normally (non-malicious). To mimic false positives during the operation of the suggested approach, random drones will be chosen. False positives shouldn't have an impact on the drones' overall authentication values. False-positive drones must recover promptly if they experience non-malicious behavior and be marked as non-malicious.

5 Results Discussion

A number of intricate situations and experiments were used to test the suggested authentication approach. The behavior of four drones (D1, D2, D3, and D4) was examined to see whether it was malicious or not. The suggested approach has been found to be capable of recognizing malicious drones that are delaying and dropping data in the IoT at 6G networks. The suggested approach also enhances the packet delivery fraction of the IoD in the absence of malicious drones, though with a reduction in the total data sent.

Therefore, this work involves defining a multi-level authentication method that can distinguish between malicious and non-malicious. The RSU is accountable for gaining authentication values in the IoD at 6G-nets. Meanwhile, 6G connections in the IoD, a ledger is utilized to keep track of these authentication values. In IoD, important communication data can be segregated from malicious drones. The suggested approach additionally preserves the integrity of the authentication value's computation. This is accomplished by making sure the information utilized to identify the authentication value is statutory.

The results demonstrate that the proposed system is successful in identifying malicious and non-malicious uavs when utilized to an internet of drone at 6G network. The proposed system improves the internet of drone authentication value, PDR, and delay in the presence of malicious uavs. The proposed system has presented some new methodologies and algorithms for determining uav behavior by assigning an authentication value to uav. The proposed system that also protects the integrity of the authentication system has been proposed.

6 Conclusions and Future Works

In this work, the security areas of IoD in 6G communications are discussed, and a multi-level authentication-based security approach is suggested.

Shortcomings of the study were discussed, along with recommendations for further investigation. In this study, will present some limitations of the study providing a direction for future research. The proposed system presented in this research was developed with a federated model and the RSUs which are responsible for investigating the presented algorithms. Nevertheless, in some environments, RSUs are not as populous. It would be beneficial to combine the suggested approach into a cloud-based scheme to increase the system's applicability and usefulness. The models and algorithms might run on a cloud server, and drones could ask it for recommendations. For instance, a uav may need to decide the better route for optimizing its path to avoid obstacles, guidance, and take off based on current weather conditions. So, processed by cloud using advanced algorithms to generate a recommendation. Drone and IoD effectiveness in the 6G network as a whole can benefit greatly by deploying and receiving information immediately through a cloud server. The implementation of the suggested approach would also benefit from a cloud-based solution. Stabilization could be pushed to every drones and RSUs through services of the cloud push no matter the position. By sent from the cloud to drones automatically data, updates, or commands instead of each drone will requested it. This confirms of all drones and devices update it by receive information or adjustments without having to manually fetch it. The suggested approach is also used with an IoD composed of drones that were either stationary or moving slowly. In the future, studies will apply the suggested approaches to an IoD composed of drones moving quickly.

Acknowledgements

The authors thank Al-Mustaqbal University as well as the head of the Al-Mustaqbal university for their financial and moral support for work.

Author Contributions

The following are the contributions made by the authors: conceptualization, Lehmoud. and Salman.; methodology, Lehmoud. and Salman.; software, Lehmoud.; validation, Lehmoud, Salman. and Joda.; formal analysis, Lehmoud.; investigation, Lehmoud.; resources, Joda.; data curation, Lehmoud.; writing – original draft preparation, Lehmoud.; writing – review and editing, Joda., Salman. and Lehmoud.; visualization, Lehmoud., Salman. and Joda.; supervision, Lehmoud., Salman. and Joda.; project administration,

Lehmoud. and Aldulaimi.; funding acquisition, Lehmoud. All authors have read and agreed to the published version of the manuscript.

References

[1] F. M. Salman, A. A. Mohammed, and A. F. Mutar, "Optimization of LEACH Protocol for WSNs in Terms of Energy Efficient and Network Lifetime," Journal of Cyber Security and Mobility, vol. 12, no. 3, pp. 275–296, 2023.

[2] P. Krishnan, S. Duttagupta, and K. Achuthan, "VARMAN: Multi-plane security framework for software defined networks," Computer Communications, vol. 148, pp. 215–239, 2019.

[3] S. Zhang and D. Zhu, "Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities," Computer Networks, vol. 183, p. 107556, 2020.

[4] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the Internet of things: A comprehensive investigation," Computer Networks, vol. 160, pp. 165–191, 2019.

[5] A. A. M. Lehmoud, N. T. Obeis, and A. F. Mutar, "Proposing a security system for the VPN through design and implementation of a scheme for android and IOS mobiles based on two-factor authentication," Periodicals of Engineering and Natural Sciences, vol. 10, no. 2, pp. 292–303, 2022.

[6] P. Bhattacharya et al., "Towards future internet: The metaverse perspective for diverse industrial applications," Mathematics, vol. 11, no. 4, p. 941, 2023.

[7] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on Deep Learning approaches for IoT security," Computer Science Review, vol. 40, p. 100389, 2021.

[8] F. M. Salman, A. A. M. Lehmoud, and F. A. Joda, " Adaptation of the Ant Colony Algorithm to Avoid Congestion in Wireless Mesh Networks," Journal of Cyber Security and Mobility, vol. 12, no. 5, pp. 785–812, 2023.

[9] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," Journal of Network and Computer Applications, vol. 161, p. 102630, 2020.

[10] F. M. Salman, A. A. M. Lehmoud, and F. A. Joda, " ESMCH: An Energy-Saving, Multi-Hop, Clustering, and Hierarchy Protocol for

Homogeneous WSNs," Journal of Cyber Security and Mobility, vol. 65, no. 6, pp. 3451–3467, 2024.

[11] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, deployments, and integration of internet of drones (iod): a review," IEEE Sensors Journal, vol. 21, no. 22, pp. 25532–25546, 2021.

[12] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," Electronics, vol. 12, no. 6, p. 1333, 2023.

[13] A. Albanese, F. Devoti, V. Sciancalepore, M. Di Renzo, A. Banchs, and X. Costa-Pérez, "ARES: Autonomous RIS solution with Energy harvesting and Self-configuration towards 6G," arXiv preprint arXiv:2303.01161, 2023.

[14] Cunha, J., Ferreira, P., Castro, E. M., Oliveira, P. C., Nicolau, M. J., Núñez, I., … and Serôdio, C. (2024). Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies. *Future Internet*, *16*(7), 226.

[15] K. A. Darabkh, A. a. B. Amareen, M. Al-Akhras, and W. a. K. Kassab, "An innovative cluster-based power-aware protocol for Internet of Things sensors utilizing mobile sink and particle swarm optimization," Neural Computing and Applications, pp. 1–44, 2023.

[16] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2241–2263, 2018.

[17] X. Cao, P. Yang, M. Alzenad, X. Xi, D. Wu, and H. Yanikomeroglu, "Airborne communication networks: A survey," IEEE Journal on Selected Areas in Communications, vol. 36, no. 9, pp. 1907–1926, 2018.

[18] Y. Zeng, Q. Wu, and R. Zhang, "Accessing from the sky: A tutorial on UAV communications for 5G and beyond," Proceedings of the IEEE, vol. 107, no. 12, pp. 2327–2375, 2019.

[19] A. Fotouhi et al., "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," IEEE Communications surveys & tutorials, vol. 21, no. 4, pp. 3417–3442, 2019.

[20] A. Sharma et al., "Communication and networking technologies for UAVs: A survey," Journal of Network and Computer Applications, vol. 168, p. 102739, 2020.

[21] Z. Ullah, F. Al-Turjman, and L. Mostarda, "Cognition in UAV-aided 5G and beyond communications: A survey," IEEE Transactions on

Cognitive Communications and Networking, vol. 6, no. 3, pp. 872–891, 2020.
[22] V. Sanchez-Aguero, L. F. Gonzalez, F. Valera, I. Vidal, and R. A. López da Silva, "Cellular and virtualization technologies for UAVs: An experimental perspective," Sensors, vol. 21, no. 9, p. 3093, 2021.
[23] R. Gupta, A. Nair, S. Tanwar, and N. Kumar, "Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges," IET communications, vol. 15, no. 10, pp. 1352–1367, 2021.
[24] M. A. Khan et al., "Swarm of UAVs for network management in 6G: A technical review," IEEE Transactions on Network and Service Management, 2022.
[25] J. Wu, W. Yuan, and L. Hanzo, "When UAVs Meet ISAC: Real-Time Trajectory Design for Secure Communications," arXiv preprint arXiv:2306.14140, 2023.
[26] I. Orikumhi, J. Bae, H. Park, and S. Kim, "DRL-based Multi-UAV trajectory optimization for ultra-dense small cells," ICT Express, 2023.

Biographies

Ahssan Ahmed Mohammed Lehmoud received his BS in computer science from the University of Babylon in Iraq in 2006. From 2009 to 2011, he completed his master's in Computer Science from the Department of Computer Science and Information Technology at Dr. BabaSahib Ambedkar Marthwada University, India. He received his Ph.D. thesis in information technology from the Department of Software College of Information Technology University of Babylon, Iraq, in April 2018. He has been a lecturer at the Babylon Education Directorate since 2008 till now. His research interests include (Information Security, Network Security, Cryptography, Steganography, Image Processing, and Data Mining).

Fadhil Mohammed Salman received his BS in computer science from the University of Anbar in Iraq in 2005. From 2010 to 2012, he completed his master's in Computer Science from the Department of Computer Science University of Babylon, Iraq. He received his Ph.D. thesis in information technology from the Department of Software College of Information Technology University of Babylon, Iraq, in 2019. He has been a lecturer at the Babylon Education Directorate since 2007 till now. His research interests include (Computer Networks, Network Security, Data Compression, Image Processing, and Data Mining).

Mohamed Q. Mohamed in Hilla, Babylon City, Iraq, on May 29, 1988, received his BSc degree in Computer Science from the University of Babylon in Iraq in 2010. He received the MSc in Multimedia in 2022 from Babylon University – Iraq. He has been a lecturer at the Babylon Education Directorate since 2012 till now. His research interests include Multimedia, Bioinformatics, Artificial Intelligence, Image Processing, and Data Mining, and Security.

Fanar Ali Joda in Hilla, Babylon City, Iraq, on November 27, 1980. He received a BSc degree in computer science in 2002 from the University of Babylon/Computer Science Dept.-Iraq. He received the MSc in Data Compression 2015 from Babylon University – Iraq. He received his Ph.D. degree in Computer Vision in 2019 from Babylon University-Iraq. Currently, Joda is Lecturer at Al-Mustaqbal University – Air Conditioning & Refrigeration Engineering Techniques Dept. His research interests include (Computer Vision and Information Hiding).

Mohammed Hasan Aldulaimi in Hilla, Babylon City, Iraq, on May 01, 1980. He received a BSc degree in computer science in 2002 from the University of Babylon/Computer Science Dept.-Iraq. He received the MSc in Knowledge Audit 2011 from University Tenaga National – Malaysia. He received his Ph.D. degree in Bioinformatics in 2017 from Universiti Kebangsaan Malaysia (UKM). Currently, Aldulaimi is Lecturer at Al-Mustaqbal University – Computer Engineering Techniques Dept. His research interests include (Information Technology, Artificial Intelligence, Knowledge Management, and Bioinformatics).